REQUEST FOR INFORMATION

Title: Office of Biometric Identity Management (OBIM) Multimodal Technology and Biometric Fusion

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY.

This RFI is issued solely for information and planning purposes; it does not constitute a Request for Proposal (RFP) or a promise to issue an RFP or Broad Area Announcement (BAA). This RFI does not commit the Government to contract for any supply or service. The Office of Biometric Identity Management (OBIM) program is not at this time seeking proposals. The issuance of this RFI does not obligate the Department of Homeland Security (DHS) in any way to issue a RFP for the goods and services described in this RFI. Responders are advised that the U.S. Government will not pay any cost incurred in response to this RFI. All costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP or BAA. If a solicitation is released, it will be via the Federal Business Opportunities (http://www.fbo.gov). It is the responsibility of the potential vendors to monitor this website for any information that may pertain to this RFI. The information provided in this RFI is subject to change and is not binding on the Government. All submissions become the property of the Federal Government, and will not be returned. In addition to the written response, the Government may request vendor capability presentations based on the scope and complexity of the RFI response. If selected, the Government will not pay for any costs associated with the presentation. Interviews can be conducted in person at the Government's facility in Arlington, VA or via teleconference.

I. Background:

OBIM operates the Automated Biometric Identification System (IDENT) for biometric matching. The current IDENT system supports daily operational decisions impacting national security and public safety. As of May 2014, the current biometric identity system stores over 169 million unique identities. The biometric gallery currently grows at a rate of approximately 2 million fingerprint records per month. The IDENT system processes more than 233,000 transactions daily for legitimate travelers to the United States, immigration benefit seekers, visa applicants, individuals seeking credentialing benefits, and persons of interest. IDENT's shortest service level agreement is providing CBP primary with a 10 second response. Currently, IDENT processes fingerprints. A limited production pilot demonstrated the capability for face and iris matching.

OBIM provides the capability for DHS and other agencies to establish an individual's identity through the capture of biometric information and associated biographic information as a risk-reduction mission under the functional mission area of people-screening. To meet this goal, OBIM provides information services to Federal, State, and local government officials to help them determine whether people are telling the truth about their identity, whether they pose a national security risk, and whether they meet the requirements for a specific government benefit. OBIM provides biometric and associated biographic identity-screening and analysis services to help decision makers reach these determinations.

To fulfill its mission and support the capability needs identified by DHS strategic planning guidance for the people-screening functional mission area, OBIM provides the following capabilities:

- Identity establishment: Using submitted biometrics and associated biographic information to uniquely distinguish an individual and connect that individual to his or her other information, such as biographic data and encounter information.
- Encounter recording: Using captured biometric and associated biographic data to record encounters and link the encounter data to an individual.
- Identity verification: Confirming the identity of an individual through the comparison of biometric and associated biographic information.
- Biometric gallery management: Creating and maintaining a biometrically based list of subjects of interest for multiple screening programs in DHS, such as for immigration violators, wanted persons, and known or suspected terrorists.
- Biometric screening: Confirming whether the provided biometric identity information matches a biometric gallery entry.
- Data sharing: Exchanging biometric and associated biographic identity and encounter information as permissible with domestic and foreign government organizations and other stakeholders.
- Data and Identity Protection: Filtering, suppressing, limiting, and managing the sharing and viewing of biometric identities and their associated encounters to ensure compliance with legal, policy, and privacy protections.

OBIM is focused on providing enhanced identity verification capabilities/services and increased interoperability, while modernizing existing operational capabilities to ensure continuous operations with no degradation in services. OBIM is also proactively addressing its next-generation architecture and capabilities. This vision represents a major investment to ensure that OBIM can continue to accommodate the expected growth of in-scope populations and new applications of biometric identity screening based on OBIM mission, effectiveness, and suitability requirements.

II. Objective:

OBIM is requesting information detailed in items a) through d) below. For each item, the respondent shall address the required technical approach including architecture, methods, tools and applicable best practices to achieve the desired objective/s. Details about technology, licensing, schemes, and costs would be helpful as well. Please **note that items are listed in decreasing priority order**.

A. **Establishment of large-scale (> 10 Million identities) matching capability for iris and face biometric modalities**: Respondents should detail state-of-the-art approaches to match these modalities against large galleries. Responses should include a description of current capabilities in terms of matcher performance and matching accuracy, as well as accuracy tradeoffs (for example between false match and non-match rates), issues in match threshold settings, and recommended uses of iris and face modalities versus Fingerprint. Further, OBIM is interested in a description of deployment and management issues associated with the above technologies. Examples of such issues would include: the general infrastructure requirements for such solutions (computing platform, connectivity, storage, any specialized/proprietary hardware, software dependencies and requirements); benchmark data for throughput; and relationships between hardware footprint, gallery size, search response time and volume of concurrent searches.

B. **Biometric fusion: Respondents should detail the state-of-the-art for multiple modalities and multiple biometric fusions and quantify the expectations for both potential advantages (increased accuracy, decreased failure-to-enroll rate, etc.) and disadvantages of various biometric fusion approaches/algorithms. Responses should contain:** details on specific implementation requirements such as software (middleware) and hardware components; impacts on response/processing time for searches; and examples of processing workflows involving the use of biometric fusion techniques.

C. **Leveraging of current OBIM multimodal data**: In addition to a limited sample for iris data from a recent production pilot, IDENT stores face images for virtually every biometric encounter (i.e. each biometric encounter includes a minimum of a set of fingerprints and a subject photo/mugshot.) While the photos do not satisfy some quality requirements for facial matching, OBIM is exploring ways to leverage this biometric data with strong privacy and security protections in place to improve the accuracy of biometric identification/verification; decrease unnecessary referrals to secondary

processing; and/or decrease the processing time of biometric transactions. Respondents should present current research on face matching with low quality, low resolution face images, and provide actual or potential case studies/examples where said images can be leveraged to improve matching operations.

D. **Assessment of current and future (3 years to 5 years) multimodal biometric technology: This section should address the following areas at a minimum**:

1) Assessment of Biometric Modalities
   i. What are the most common biometric modalities and which modalities are likely to see an increase/decrease in usage and/or acceptance?
   ii. For the different modalities, what are the state-of-the-art technologies and the corresponding match and error rates?
   iii. What are the characteristics of the different modalities that should be considered that might make one more/less advantageous or more/less desired over the others?
   iv. What are some guidelines and criteria for capturing each of the modalities to ensure they can be utilized for matching operations and decrease the likelihood for mismatches and failed transactions?
2) Implementation considerations:
   i. What modalities best support an approach to maximize commodity components and use of COTS software and hardware?
   ii. What product vendors' best support an approach to maximize commodity components and use of COTS software and hardware?
   iii. What tradeoffs should be considered when attempting to build a large scale biometric matching infrastructure?
   iv. Given requirements for rapid matching, what technical approaches exist to provide the necessary performance at scale? (Assume rapid matching requires response times of less than 10 seconds with gallery sizes of 1,000, 100,000, 10,000,000, 1,000,000,000, etc.)
   v. Are there services that can be bought on a subscription basis without the Government building its own infrastructure (such as current or future cloud-based matching service)? What are the advantages / disadvantages in terms of cost, scalability, security protocols, elasticity, performance, etc?
   vi. For each modality, what is the best/desired image resolution given practical constraints of storage; ease of image capture; and network bandwidth considerations?
   vii. What are the different licensing models used for biometric matching software and hardware? What license model is the most advantageous to the Government? Is there a licensing model that would be least advantageous to the Government's interest?
   viii. What are the data and Identity Protections in place - to include filtering, access controls, suppressing, limiting, and managing the sharing and viewing of biometric identities and their associated

encounters to ensure compliance with legal, policy, and privacy protections?

III. Submission:

Interested parties shall follow submission instructions posted on the FedBizOpps notice with this RFI announcement.

Note: Non-government staff support personnel will not have access to RFIs labeled by the submitters as Government Access Only.

A. This notice is for market research and planning purposes only and does not commit the Government to any contractual agreement. This is not a request for proposal. The Government does not intend to award a contract based on responses under this announcement nor otherwise pay for preparing any information sent for the Government use. Any submission will become the property of the Government and will not be returned to the submitter.

B. Email instructions are posted on FedBizOpps with this RFI announcement.

Submissions in Section II A through D shall not exceed 50 pages, including a cover page and a one page executive summary.